

Informacje o chorych na otwartym serwerze

BEZPIECZENSTWO Każdy, kto chciał, mógł skopiować niezabezpieczone żadnym hasłem dane osobowe 50 tys. pacjentów szpitala w Kole. Sprawę zbada GODO

Sławomir Wikariak
slawomir.wikariak@infor.pl

Wystarczyło znać adres IP serwera Samodzielnego Publicznego Zakładu Opieki Medycznej w Kole, by mieć niczym nieskrępowany dostęp do przechowywanych na nim plików, w tym bazy danych osobowych 50 tys. pacjentów. Każdy mógł poznać ich imiona i nazwiska, adresy zamieszkania, numery PESEL i ubezpieczenia, a także grupę krwi. Ale to nie koniec. W jednym z plików zapisano dane dzieci wraz z informacjami na temat chorób zakaźnych, jakie przeszły. W innym katalogu były personalia 600 pracowników szpitala, a w kolejnym – numery ich rachunków bankowych.

Będzie kontrola

Bulwersującą sprawę opisał w poniedziałek serwis Zaufana Trzecia Strona, który o niezabezpieczonym serwerze dowiedział się od jednego z czytelników. Sprawdził doniesienie i na dowód tego, że jest prawdziwe, zamieścił w sieci zrzuty ekranowe plików z zamazanymi danymi pacjentów.

– Wszystko wskazuje na to, że mieliśmy do czynienia z błędem człowieka, który pozostawił serwer niezabezpieczony. Nie wiadomo, jak długo dane były na nim przechowywane ani kto miał do nich dostęp. Wiadomo natomiast, że w ogóle nie powinny się znaleźć na serwerze udostępnionym w internecie, nawet prawidłowo zabezpieczonym. To dane wrażliwe, należy je trzymać w systemie medycznym – mówi proszący o zachowanie anonimowości redaktor serwisu Zaufana Trzecia Strona. Poinformował on szpital o braku zabezpieczeń i związanym z tym zagrożeniem. Po tym powiadomieniu dane zostały zabezpieczone, ale... jeszcze przez

kilka dni możliwy był dostęp do podglądu folderów.

DGP zapytał dyrekcję szpitala, w jaki sposób doszło do udostępnienia plików z wrażliwymi danymi w internecie, ale do zamknięcia wydania nikt nie udzielił nam odpowiedzi.

Głos zabrało za to Biuro Generalnego Inspektora Ochrony Danych Osobowych. – Choć sprawę znamy jedynie z doniesień medialnych, to biorąc pod uwagę skalę wycieku i charakter danych, które były publicznie dostępne, GODO postanowił zająć się nią z urzędu – informuje rzecznik prasowa Agnieszka Świątek-Druś.

Zwraca ona uwagę, że w przypadku ujawnienia dokumentacji medycznej w grę wchodzi nie tylko naruszenie ustawy o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922 ze zm.), ale także przepisów regulujących funkcjonowanie placówek opieki zdrowotnej. Chodzi m.in. o ustawy o: prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz.U. z 2016 r. poz. 186 ze zm.), systemie informacji o ochronie zdrowia (t.j. Dz.U. z 2016 r. poz. 1535 ze zm.) czy wreszcie zawodach lekarza i lekarza dentysty (t.j. Dz.U. z 2017 r. poz. 125 ze zm.). Ta ostatnia ustanawia tajemnicę lekarską, z której złamaniem mogliśmy mieć do czynienia w tym przypadku.

Możliwe zadośćuczynienie

Postępowanie prowadzone przez GODO może skończyć się skierowaniem do prokuratury zawiadomienia o złamaniu prawa przez administratora, za co grozi kara do dwóch lat więzienia. Szpital musi też liczyć się z odpowiedzialnością cywilną.

– Osoby, których dane zostały udostępnione, mogą domagać się zadośćuczynienia za naruszenie dóbr osobistych. W praktyce sądy w tego typu sprawach

Skutki złego zabezpieczenia danych

10 MLN EURO

72 GODZ.

50 TYS. OSÓB

mogło ucierpieć w wyniku braku zabezpieczenia dostępu do ich danych osobowych przez szpital w Kole

kary będzie od maja 2018 r. grozić firmom, które nienależycie zabezpieczają dane osobowe i umożliwiają ich wyciek

będzie miał od maja 2018 r. administrator na zgłoszenie wycieku danych osobowych

nie zasądzały zbyt wysokich kwot, co do zasady mieszczą się one w przedziale od 7 tys. do 10 tys. zł. Tu jednak mamy do czynienia z informacjami wrażliwymi, a więc dotyczącymi sfery najbardziej intymnej, co pewnie mogłoby wpłynąć na wysokość orzeczonej rekompensaty – wyjaśnia Marcin Cwener, ekspert prawny z Omni Modo.

Sytuacja prawna zmieni się w maju 2018 r., gdy zacznie obowiązywać nowe unijne rozporządzenie 2016/679 o ochronie danych osobowych. Wówczas poszkodowany będzie miał dwie drogi dochodzenia roszczeń. Jedną to wspomniane już przepisy cywilne dotyczące naruszenia dóbr osobistych, zaś drugą podstawę będzie dawać wprost unijne rozporządzenie.

– Nie wykluczam, że pójście tą drugą ścieżką może być korzystniejsze dla osoby, której dane wyciekły. Ponieważ rozporządzenie przewiduje mi-

lionowe kary finansowe, sąd poprzez analogię może uznać, że zadośćuczynienie powinno być wyższe niż na zwykłej drodze cywilnoprawnej – tłumaczy Marcin Cwener.

Szpitala poza ustawą

Maksymalna wysokość kar za wyciek danych wyniesie 10 mln euro. Jak wynika jednak z projektu polskiej ustawy wdrażającej te przepisy, nie zostaną nią objęte publiczne szpitale (ale prywatne już tak). Wszystkie natomiast będą musiały jak najszybciej informować osoby, których dane wyciekły. Dzisiaj przepisy nie nakładają takiego obowiązku.

– W ocenie GODO powiadomienie osób, które na skutek wycieku danych zostały poszkodowane, byłoby dobrą praktyką, jako że byłyby one poinformowane o samym incydencie i poczone, jak mogą w tej sytuacji postąpić – komentuje Agnieszka Świątek-Druś.